Assurance Protocols and Small Web Retailers

G.E. Lyon
Distributed Systems Technologies Group
High Performance Systems and Services Division
National Institute for Standards and Technology
100 Bureau Drive Stop 8951
Gaithersburg MD 20899-8951
1-301-975-5679
lyon@nist.gov

ABSTRACT

Many Web areas are in an early technological period of rapid evolution and intense competitive selection. Nowhere is this truer than with electronic commerce. While much is being considered today for business-to-business transactions, the Web also represents a marvelous opportunity for small retail establishments. However, the needs of small establishments differ from those of larger firms. In particular, customer assurance is very important. Several assurance protocols are examined for their utility to small retail sellers on the Web. One new possibility involves using bankcard records to build assurance ratings.

Keywords

Assurance; customer; e-commerce; implementation; seller; verifier; World Wide Web.

1. INTRODUCTION

The Internet and its architecture have evolved in a rapid and sometimes chaotic manner. It has been stated, with perhaps some hyperbole, that “The Internet is the largest engineering undertaking ever, and it is evolving without a grand design blueprint.”[3]. The scale of the Internet is definitely sprawling, but whether a grand design is possible, or even desirable, is an open question. In many respects the Internet has characteristics more in common with national highway systems, aviation commerce or urban developments than with conventional, closed-participation software projects, whatever their scope. One thing that emerges with urban development is a set of architectures specific and local to their circumstances. Certainly, common design elements are often successfully shared among similar applications. Nonetheless, who has ever seen two identical airports or cities? The sources of design divergence are simply too rich, the advantages of shared, common designs not obvious. The economics of one Web application may not work for another that appears to be nearly identical.

SAC’00 MARCH 19-21 COMO, ITALY

2000 ACM 1-58113-239-5/00/003

Many Web areas are in an early developmental stage of rapid evolution and intense competitive selection very reminiscent of early computer language developments decades ago. Nowhere is this truer than in electronic commerce. The pace in e-commerce is swift. And, while most e-commerce services being considered today are for business-to-business transactions, the Web also represents a marvelous opportunity for small retail establishments. Internet connections make possible sales far removed from a shop's physical location, which can be quite rural. All that is required is adequate telephone service. However, some needs of small establishments differ from those of larger firms. Small firms are usually unknown entities to potential customers, so customer assurance is of paramount importance. Several assurance protocols will be examined for their utility to small retail sellers on the Web.

2. ASSURANCE PROTOCOLS

Purchasing via the World Wide Web can trigger considerable customer anxiety. This angst is not unfounded [8]. An electronic virtual world, like smoke and mirrors, is easily manipulated. J. Schoenfeld, CEO of Net Effect, says only 5.75 percent of Web site visitors even attempt to purchase something and that 67 percent of online purchases are aborted. Her observations come from a five-month study covering two dozen network enterprises. In the Web marketplace, an unfamiliar vendor suffers significant disadvantage. Customer reluctance persists even when the network is known safe. The true issue for a would-be buyer is whether the seller is *bona fide*. For example, are premises of the establishment dusty and ramshackle or modern in appearance? Network customers cannot make physical inspections of a business to allay their doubts.

The issue of assurance becomes especially pronounced when a potential supplier *appears* highly attractive over the network but remains a completely unknown entity. Smaller businesses often fall into this category, which is unfortunate. Small businesses can be especially vigorous and competitive. They are numerous--in the United States, firms with fewer than 500 employees employ about 53 percent of the commercial work force. These businesses contribute 47 percent of all U.S. sales and 51 percent of the U.S. GDP (figures from U.S. Departments of Commerce and Labor via www.nsbu.org). If customers can be made more confident, Web commerce represents an ideal place for small firms to thrive.

Appears in: Proceedings of the 2000 ACM Symposium on Applied Computing, Como, Italy, March 19-21, 2000, pp. 904-908.

ASSURANCE PROTOCOL	SUBJECTIVE SCORE	REL. COST/TRANSACTION (EST.)
None	Uneasy (-1)	0
Simple Acknowledgment	Confirmed (+1)	1
Query-Based directly after sale	Confident (+3)	10
Audit-Based	More Confident (+4)	10 (heavy use) to 100+ (light use)

Table 1. Marks for Four Types of Assurance Protocols

1	Customer C to Seller S	Inquiry via Web (includes payment)
2	Seller S to customer C	Sales completion—merges into step 4
3	Seller S to verifier V	Assurance provider notified
4	Verifier V to customer C	Inquiry on sales transaction
5	Seller S to customer C (later option)	Inform on details of shipment
6	Verifier V to customer C (later, still)	Query customer on quality of experience and purchase(s)

Table 2. Typical Use of Query-Based Protocol

2.1 Assuring the Uneasy

An assurance protocol is designed to dispel wariness toward a new party. Social instruments such as letters of introduction play this role in everyday life. A Web-based assurance protocol should function analogously to build trust (examples include [4] and [12]). Discussion begins with several simple types of assurance protocols for Web retail sales. Emphasis is upon levels of assurance versus cost per transaction: A large business-to-business transaction can tolerate more cost overhead than can a Web retail sale for $19.

2.2 No Confirmation

Suppose customer *C* wishes to interact with a reliable seller *S* somewhere in the virtual world of the Web. C is unsure whether S is such a supplier. Exchanges can be made among C, S and a third party *V* who may, in varying degrees, vouch for the authenticity or reliability of S. The most unsatisfying of C's Web-purchase transactions occurs when the customer completes a Web purchase and there is no further response from S until the merchandise appears (or worse, does not appear). Ill ease descends upon C and lingers until S delivers the product. Even then, C has residual smarting about the purchase. Such behavior by S is gauche but is easily found on the Web. Table 1 depicts this circumstance in its first row, where a subjective grade or mark of –1 has been assigned to "uneasy." The cost to seller S (third column, row 1) is zero, since no assurance has been given to C. In actuality, there is another cost for this negligence—customers who find a more communicative site will readily abandon S.

2.3 Simple Acknowledgment

A more polite seller acknowledges an order with e-mail shortly after the automated Web session. This small but effective gesture indicates something is actually happening–it is as assuring as a failure to confirm is discouraging (the respective marks being +1 and -1 by the grading scheme—cf. Table 1). Confirmation cost is higher than doing nothing, but it is still slight.

2.4 Query-Based

Table 2 gives a scenario with a query-based assurance protocol. This scenario begins with customer C being unfamiliar with the URL for finding the query-based assurance information. (The other case follows in section 2.6.) In Table 2, a purchase is initiated without prior assurance (Table 2, rows 1 and 2). However, in closing out the transaction, the assurance provider (or a proxy) questions the customer (step 4) and mentions a later, follow-up session. This raises customer confidence considerably more than a simple confirmation (+3 in Table 1). The next working day or so, the seller may further contact C (step 5, Table 2) with details such as shipping schedules, carrier and invoice number. This again improves confidence. Later still (step 6) the verifier *V* queries on the overall quality and satisfaction of the transaction. While not pertinent to the sale (goods have arrived by now), this action again increases the customer's confidence in S. Repeat sales are more likely. Customer responses go automatically into V's vendor database. Digests of responses are also incorporated into a Web public rating list maintained for use by the public.

1	Verifier V to Seller S (earlier)	Certificate to seller; several months lifetime
2	Customer C to Seller S	Initial inquiry via Web
3	Seller to customer	Web response (incl. certificate)
4	Customer to seller	Purchase details (incl. payment)
5	Seller to customer	Automatic confirmation

Table 3. Audit-Based Assurance Protocol

1	Customer C to Verifier V	Inquiry on seller's standing; open rankings; free.
2	Step 1, Table 2 above	Balance of transactions as per Table 2

Table 4. Prior-Use of Query-Based Information

1	Customer C to Verifier *V* *Alt: C to S directly*	Background check on seller; use closed proprietary files on bank card payouts; has general metrics (below)
2	Verifier *V* to Customer *C* *Alt: S to C*	Rating of seller *S* based upon credit-card volume, logged complaints/volume, other business indicators *Alt: send certificate on most recent BCI rating*
3	Customer C to Seller S	Order via Web; includes payment
4	Seller S to Customer C	Sales confirmation

Table 5. Using Bank Card Information (BCI)

2.5 Audit-Based

Table 3 depicts another protocol approach that is audit-based. This mechanism is structured very similar to common accounting practices. An accountant (part of the verifier V here) audits supplier S and finding satisfactory conformance to principles of good electronic commerce, issues an electronic certificate valid for a fixed period, usually several months (step 1). Customer C subsequently sees this certificate during an inquiry (step 2) and gets further details (step 3). The audit-based seal of assurance is managed by a third party. Assured by reading the certificate, C makes an order (step 4) and receives confirmation (step 5). The process seems fairly effective, although accountants have some reluctance about management (and knock-off copying) of the approval seal. They also worry about legal liability attending their endorsements.

Periodic audits required for retaining the seal add considerable expense. A large-volume seller will incur a far lower cost per sale for assurance overhead than will smaller retail merchants. With heavy use, audit-based might be similar in cost to query-based (both are rated 10 in Table 1, third column). However, light use of audit-based assurance will render the per-sale overhead very high (100+). The good thing is that assurance comes at the start of the Web session—this should help stem the loss of those two-thirds of Web sales that are aborted.

2.6 Query-Based Revisited

An alternate use of query-based assurance has customers going first to public rating Web pages. Table 4 shows the beginning of this. An early check with V gives customer C an assurance similar to audit-based approaches. The cost of this should be relatively low, since collection methods can be highly automated. Another advantage is its incremental nature. It avoids sometimes expensive periodic audits. However, with few sales and likelihood of many customers skipping the query-based rating form, the smaller merchant may suffer a significant disadvantage. A query-based assurance provider may have only 50 sellers in its music category for the whole U.S.A. When response numbers are too low, some of these rankings may be based upon staff investigations rather than regular responses. Imagine if the list got to be 100 to 200 times longer, with many entries having only a few tally points. Clearly, scalability of the mechanism can be a challenge when the number of sellers becomes quite large and a good fraction of these additional merchants do only a tiny amount of Web business.

2.7 Umbrella Organizations

E-commerce organization may diverge from conventional retailing. Nothing illustrates this better than a Web umbrella or virtual store supporting merchants—manufacturers, distributors, retailers–of all sizes. Reference [11] describes an example.

Typically, each participant must (1) sell products that ship via some convenient means and (2) provide suitable catalog descriptions of their product line. The umbrella store may host most transactions and customer services, running a business's Web pages, collecting payments and ordering shipments. Participating stores and the umbrella store receive commissions on sales. Customer assurance comes from dealing through the umbrella store, a "digital intermediary" [1]. This is attractive in many ways. For one thing, the host is a known entity. Lack of seller name recognition also poses much less a problem, since the participant seller S works under the mantle of the virtual store's implied and express guaranties. For instance, buyers at umbrella stores are typically given a shopping warranty--any unauthorized bankcard charges are covered, up to the buyer's limit of liability, which is $50 in the U.S.A. In a sense, the verifier V and the seller S are combined under the umbrella store; seller S is actually a store affiliate paid commissions on sales by the parent organization. Seller commissions range from 5 to 25 percent, depending upon the merchandise.

One major reservation is the business efficiency of shops in a virtual store. Like the small shop in a massive shopping mall, the size of commissions paid out to the umbrella organization may prove nettlesome to a Web seller's profitability. For example, American merchants are never happy with the three to five percent of sales that they must pay for credit card handling. Another question arises about the uniqueness of the various stores—are they essentially offering the same goods and services available from any of their rivals? That said, the umbrella store is a new, engagingly fresh application architecture; it approaches the question of small seller trust assurances from a completely different angle. Time will tell how it succeeds.

3. A NEW APPROACH, BCI

Lessons from the foregoing examples can be summarized as:

(1) Supply assurance early-on to hold sales
(2) Design a simple, fast assurance mechanism–one amenable to automation
(3) Have the mechanism scale down for size of operation (boutique vendors) and up on number of sellers (thousands)
(4) Eliminate most human participation, e.g., no customer response forms.

Item (1) follows from the discussion on behavior of would-be Web shoppers. Items (2) and (4) define a mechanism cheap to run. Item (4) also mentions a source of statistical unreliability—the use of voluntary responses. Merchants with few customer sales will have even fewer tallied evaluations. The statistics for assurance may be shaky. Item (3) specifies good scalability. As discussed earlier, a tabulation of customer comments is fine for large retailers with name recognition and a large volume of sales. It is unclear how well this works when the merchant list comprises several thousand names, many of which are unfamiliar.

Table 5 sketches a new assurance approach, *BCI* (BankCard Information), that addresses items (1) through (4) above for small, competitive but unknown vendors. Customer C first invokes an automated background checker from a browser. This background is based upon information that is implicit in any bankcard-based sales seller S has made in the past. The check is performed by a credit card organization V *upon* seller S's records without S knowing who has made the request. The service V reports back upon the seller's viability and standing among the credit card user community. Indicators might include the seller's level of activity (transactions/day), complaints/sale and other similar metrics. There are no forms for customers and participation by sellers is voluntary.

The approach inverts the usual credit association, where business S checks upon buyer C. Here, customer C checks (electronically) upon the seller's business standing via credit-card payment records. Since these might come from many different banks, the payments could be logged locally and aggregated by the verifier V on a periodic basis. Daily updates of the ratings seem unnecessary—a weekly update cuts the overall effort and allows the load to be staggered. Special updates can be made when a rating changes drastically. Many confidential details can be masked while still providing the necessary indications for assurance. Bypassing a manual audit and assessment, the approach should be less costly than audit-based assurance. It would automatically qualify every Web-based merchant, since bankcards are one of their principal methods of payment. Merchants will also appreciate that their local established bankcard trade contributes to their Web assurance standing. That is, a rural seller with a sterling local reputation will have this reflected immediately in his Web assurance rating, even before he has sold anything through e-commerce channels. This "auto-start" reputation is attractive.

Customers would not necessarily have to make their assurance request to verifier V. The rating could be reissued weekly or monthly much like the audit-based seal of assurance in Table 3, step 1 (using the same security mechanisms) and posted at the seller's Web site. This would disperse assurance inquiries away from the verifier, V and thereby promote better scalability. Another simplification would be for the verifier V to issue assurance seals in only a few types, like investment ratings. An excellent merchant would be rated A or AA, a lesser one B, and so on. This would allay sellers' questions about outsiders getting digests of their firms' business. The seller would pay the verifier for the rating service. Provided the banks and card issuers handle the needed archival files efficiently, cost should be considerably less than audit-based aussurance. BCI would be highly automated.

4. FURTHER RELATED DIRECTIONS

BCI might qualify as a future topic in studies of how unknown entities such as small shops or Web customers might authenticate and validate crucial information in transactions over the Internet. Imagine each entity has links to its own sponsor institution--a bank would be typical in America, but in other countries the Post Office might be a natural candidate. Assume that pairs of transacting entities have no authentication means common between them. They will rely instead upon their financial/informational proxies to provide secure, anonymous transactions and to guarantee payment and shipment obligations. One example of a recently begun study along these lines is FAST[6].

Customer and merchant negotiate with each other over the Internet. Each then authorizes its representing institution to exchange, authenticate or assure the more sensitive elements of the transaction with the counterpart institution. The set of possible transaction elements is considerably broader than the simple ratings proposed for BCI, and it illustrates where the future might lead. For example, one might want to authenticate citizenship, marital status, education, membership and licensing standings via electronic means [6]. On an even broader front, other parties have expressed an interest in linking authentication and assurance with Internet-based manufacturing functions [10]. Items of concern include an environment that securely transacts international finances or that ties payments to manufacturing achievements. Continuing beyond this, a NIST colleague suggests checks on legal matters would serve well in some lines of business—this includes indictments, lawsuits brought by and against the entity in question, criminal records, civil judgments and related settlements. This partial enumeration of desired yet sensitive information signals a definite need to mention privacy [9].

5. QUESTIONS OF PRIVACY

Implicitly or explicitly, privacy always remains an element in the design of commercial systems. While it is beyond the scope here to explore privacy with any thoroughness, a few remarks will highlight typical problems. Privacy can have dimensions that are technical (security), policy (trust) or economic (cost and profit) in flavor [7]. On the technical side, there is always a tradeoff between security and cost. Even excellent security protocols will have to survive a business case analysis. Public key methods are probably too complex for most small Web retailers. Other approaches for secure electronic transactions have proven somewhat expensive and failed the business case: U.S. merchants find it cheaper to absorb losses incurred with lesser levels of protection than to use more secure but costly protocols.

5.1 Trust and Profit

Banks in the United States traditionally have fulfilled many community trust responsibilities. The quaint names for some establishments, such as “Farmers and Mechanics Bank and Trust,” attest to this fact. Today, however, banking is experiencing a period of rapid transition. Many banks have become large aggregates of regional, national or international sweep. Recent U.S. federal legislation allows banks to sell insurance and stocks. Even before this development, privacy lapses within banks served to illustrate pressures on modern businesses [2]. This pressure, along with the enlarged scope of banking enterprises, will generate further temptations to blur trust functions with other profit opportunities [5]. For this reason, institutional policy commitments on privacy are as important as any technical approaches.

6. CONCLUSIONS

Assurance methods are perhaps a metaphor for network commerce today. Early assurance efforts have attempted to merge older practices (acknowledgments, customer surveys, and audits) into Web technology. Several of these assurance protocols have been evaluated for their cost and effectiveness for small retail merchants. The evaluation shows that one might want a protocol with (1) assurance given early, (2) a fully automated data collection scheme, (3) system scalability, and (4) no crucial human intervention. Requirements (1) through (4) suggest a new approach, BCI, an assurance method based upon bankcard information. BCI may offer attractions for small firms. However, e-commerce is new and unpredictable. Emerging architectures like the umbrella store could change the scene completely. Searches for efficient e-commerce architectures will continue for some time as the various technical elements adjust to market forces.

7. ACKNOWLEDGMENTS, REMARKS

Thanks go to Alan Mink of the Distributed Systems Technologies Group for comments and suggestions.

Contributions of the National Institute of Standards and Technology are not subject to U.S. copyright. Mention of commercial products or services is only for illustrative purposes and should not be taken as an endorsement, express or implied.

8. REFERENCES

[1] Ba, S., Whinston, A. B. and Zhang, H. Small business in the digital economy: Digital company of the future. Proceedings of the Conference on Understanding the Digital Economy: Data, Tools and Research (Washington, D.C. 1999), MIT Press [to appear]. http://www.digitaleconomy.gov

[2] Barncik, S. OCC’s Chief Counsel warns banks to shield data privacy. American Banker (October 7, 1999) 2.

[3] Benda, M. Internet architecture: Its evolution from an industry perspective. IEEE Internet Computing 2, 2(March-April 1998), 32-35

[4] BizRate.com® reference text. http://www.BizRate.com

[5] Dugas, C. Banks sell your secrets: Account numbers, names, addresses are all fair game. USA Today (October 21, 1999), 1B.

[6] FAST project of the Financial Services Technology Consortium. http://www.fstc.org

[7] Ghosh, A.K. E-Commerce Security. John Wiley & Sons, Inc., New York NY, 1998.

[8] Gray, G. L., and Debreceny, R. S. Electronic commerce assurance services and accounting information systems: A review of research opportunities. Advances in Accounting Information Systems 6, (1998), 185-206.

[9] Penenberg, A. The end of privacy. Forbes 164,13(November 29, 1999), 182-189.

[10] Talley, M. Memorandum to FAST Project on initiatives of the National Center for Manufacturing Sciences, October 21, 1999.

[11] Vstore.com organization. http://www.vstore.com

[12] WebTrust™ description text.
http://www.aicpa.org/webtrust/into.htm.

Biographical Sketch

Gordon LYON manages the Distributed Systems Technologies Group at the National Institute of Standards and Technology, Gaithersburg, MD. He joined NIST in 1972 upon completing a Ph.D. in computer science from The University of Michigan. Prior to NIST, Lyon worked in advanced applications prototyping at the General Motors Research Laboratories and in human performance at The University of Michigan Medical School. Primarily interested in non-numerical programming techniques, Lyon has contributions in the areas of syntactic pattern recognition, scatter storage, programming languages, programming environments, and performance measurement tools. He is a member of ACM, IEEE Computer Society, and SIAM.